INFORMATION SECURITY:

SECURING SMART CARDS WITH IRIS RECOGNITION

THESIS

Orval E Phelps, Captain, USAF

AFIT/GIR/ENG/01M-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U. S. Government.

AFIT/GIR/ENG/01M-01

INFORMATION SECURITY: SECURING SMART CARDS WITH IRIS RECOGNITION

THESIS

Presented to the Faculty of the Graduate School of Engineering and Management
of the Air Force Institute of Technology
Air University
Air Education and Training Command
In partial Fulfillment of the Requirements for the
Degree of Master of Science in Information Resource Management

Orval E. Phelps, B.S.
Captain, USAF

March 2001

Approved for public release, distribution unlimited

AFIT/GIR/ENG/01M-01

INFORMATION SECURITY: SECURING SMART CARDS WITH IRIS RECOGNITION

Orval E. Phelps, B.S.

Captain, USAF

Approved:

Henry B. Potoczny

Henry B. Potoczny, PhD

Feb. 28, 2001

date

Gregg H Gunsch

Gregg Gunsch, PhD

28 FEB 2001

date

Michael G. Morris, Major, USAF, PhD

28 FEB 01

date

Acknowledgements

I would like to express my appreciation to my academic advisor, Maj. Michael Morris, Ph.D., my thesis reader, Dr. Gregg Gunsch, and my thesis advisor, Dr. Henry Potoczny, who provided invaluable guidance in this thesis.

I wish to express my appreciation to Dr John Daugman, at the University of Cambridge, who provided invaluable assistance in providing me with scientific papers and up-to-date information on the technology studied here.

Thanks also to the AFIT GIR01M class for their assistance during the program. The moral support and teamwork in class made the program better and the load lighter.

A word of thanks to U.S. General Services Administration (GSA), Office of Governmentwide Policy, Office of Electronic Commerce and to my point of contact Bill Holcombe for agreeing to sponsor this thesis. By sponsoring my work, it made it that much more valuable and provided me greater incentive to do well.

Lastly, thanks goes to my family, whose selfless devotion and support during the past 18 months allowed me to focus on my studies in this graduate program. Without their support in this endeavor, it would not have been accomplished.

Table of Contents

List of Tables

AFIT/GIR/ENG/01M-01

Abstract

This thesis examines the application of iris recognition technology to the problem of keeping smart cards secure. In order to understand the technology, a comprehensive literature review was conducted. The biological components of the iris were examined to ensure that they were truly random in development and static through the lifetime of the individual. Specifically, the physical structure of what comprises the iris was examined in detail. The data gathered indicates that the iris is formed early in development, random in structure, and stable throughout the person's lifetime.

Next, the iris recognition process and resulting recognition code was examined to determine how it could be used. Examination of methods to eliminate counterfeit codes and the randomness of independent codes was vital. Statistics on reliability of the iris recognition process were also examined. Iris recognition was found to be exceptionally reliable, difficult to counterfeit and fast to use.

In order to ensure security, the cryptographic strength of the iris recognition code was examined. It was necessary to determine the time necessary to break the iris recognition code should the smart card be compromised. Due to the randomness of the code, exhaustive searches are the only viable means of breaking the code and the time durations to accomplish this are excessive.

Additionally, smart card technology was examined to determine if existing technology could store the necessary iris recognition information for use in identity verification. Current processing ability and storage requirements of smart cards exceed the minimum requirements for use of iris recognition technology.

The conclusion of this thesis is that iris recognition technology is a viable means of securing smart cards against unauthorized access with high reliability, confidence and speed.

INFORMATION SECURITY: SECURING SMART CARDS WITH IRIS RECOGNITION

I. Introduction

There is a large amount of information accessed and protected every day. There is a constant demand for briefcases with good locks to protect the medical records or secure documents that people need to carry. People, because of the constant need for this information, constantly carry address books, date books, password lists, and other sensitive data. There has been a need to consolidate this deluge of information into a compact and secure storage device for daily access. The computer industry has been working diligently to try to develop a storage technology that is compact and secure for some time and has arrived at some very useful solutions. The U.S. General Services Administration (GSA), Office of Governmentwide Policy, Office of Electronic Commerce is tasked with investigating some of these problems and solutions and sponsored this study (Holcombe, 2001).

Smart cards, intelligent data storage devices, are beginning to come into use as a form of identification and authentication. According to Webster, a smart card is "a small plastic card that has a built-in microprocessor to store and process data and records" (Webster, 2000). These smart cards can contain personal data, cryptographic keys, and other sensitive data stored in a compact and secure form. The government is currently examining uses for this technology within its various components, particularly the Department of Defense. For example, the Department of Defense Access Card is being developed to control physical access to facilities and store cryptography keys for use in public key cryptography systems (SmartGov, 2000). One of the inherent problems with smart cards is the possibility of loss or theft of the smart card. This loss or theft can make unauthorized use a possibility and therefore requires protection mechanisms to prevent this occurrence. Current options for securing smart cards against unauthorized use are primarily restricted to passwords. Passwords rely on procedures to ensure they are strong enough to protect the token but easy enough for the user to remember so that they do not resort to writing them down. Passwords are generally relatively short and are highly vulnerable to brute force cracking mechanisms. Size restrictions on password lengths limit the security of a password protection system greatly. Changing passwords on a regular basis is vital to maintain the security of the system, but this complicates the ease of use since the user constantly has to remember a new code. In addition, passwords are restricted to a subset of the complete character set which reduces the number of possible passwords.

Biometrics offers another protection solution for smart cards. Biometrics is the statistical analysis of biological observations (Webster, 1996). Biometric identification systems use a biological component, such as an eye, face, or voice, as a method for recognizing a person by measuring one or more specific physiological or behavioral characteristics, with the ultimate goal to distinguish that person from all others. In this sense, a biometric identifier takes a biological feature and uses it as a token for access. A biometric identifier is always with the individual and is difficult to duplicate. It is impossible to write down and it cannot be lost with the card. A good biometric does not change frequently, cannot be damaged easily, is unique for each individual, is simple to use and can be encoded efficiently and securely. Although there are many different biometric mechanisms available, such as fingerprints, retinal scans, face recognition, and voice recognition, the human iris appears to present the best option for a viable and safe biometric identifier. Other highly reliable biometric identifiers, such as DNA, require physical contact and are not as safe as identifiers used at a distance (Buda, 1999; Daugman, 1998).

IriScan, Inc. has developed a biometric identification procedure using iris patterns to generate a unique access code based on the encoding methods of Dr John Daugman of the University of Cambridge in the United Kingdom. They own the specific methods used and license this technology to other companies to expand the range of applications where it can be used. This method is non-intrusive and has the potential to replace passwords for securing smart cards. The IrisCode^{TM} generated by the IriScan, Inc. software is large and complex enough to resist various code breaking methods and small enough to fit on smart cards. Currently, IriScan, Inc. is working on pilot projects that use iris recognition technology for securing smart cards in response to industry and government demands to select good biometrics to protect smart cards.

The Smart Card Technology Center, a multi-agency program (MAP) between the General Services Administration (GSA) and the Navy to foster smart card standardization and interoperability, is working on some applications for non-contact access, digital signatures, expanded biometrics, financial processing/ATM capabilities, portable readers, warrior readiness and an interactive kiosk. Iris recognition is a means of non-contact access and identification. Industry is providing inputs to this organization with suggestions for solutions to the access control of smart cards (SmartGov, 2001).

Pursuant to these government needs, this thesis examines the non-contact biometric iris recognition as a means to secure smart cards against unauthorized use. This thesis studies the feasibility of using iris recognition technology to secure smart cards. This is accomplished by examining the biological foundation of the technology, cryptographic security of the generated iris recognition code and the feasibility of securing a smart card using this technology. The results of this study will demonstrate the security, usefulness, and affordability of implementing iris recognition to the security of smart cards used by the Department of Defense thus eliminating the need for passwords in many areas.

II. Research Methodology

A case study approach is useful in examining technologies where the data is in archival form. This form of methodology is well suited to this thesis since the data collected is from the comprehensive literature review of the subject. The technologies explored here are rapidly evolving. The data necessary to evaluate and draw conclusions is available both in the literature and through personal correspondence with the developers of the technologies. This thesis most closely resembles the *Case Studies of Medical Technologies* done between 1979 and 1981. These are primarily technology assessment studies that aided decision makers in deciding what they needed to do concerning various medical technologies. Most of the data for those studies was gathered from archival analysis. This thesis takes a similar approach and deals with assessing the iris recognition and smart card technologies and determining if these technologies can be used together securely (Yin, 1984).

Phase One – Biological Basis

Phase one was the evaluation of the biological basis for iris recognition. This involved examining the properties of the iris. Those properties of interest included the unique development of the iris pattern, the stability of the pattern over time, and the effects of eye surgery and other corrective measures on the pattern as reported by expert opthamologists.

Review of medical texts provided the data gathered on the biological properties. The iris properties, its structure, and its development are firmly established in medical literature. The unique development of the iris was critical to this study. The effects of the environment and stability of the iris structure were important concerns. In addition, eye surgery and other corrective medical techniques required examination to determine their impact on the iris.

Phase Two - Technology

Phase two involved explaining the technology developed by John Daugman, Ph.D. and owned by IriScan Incorporated, which takes an image of the iris and converts it into a code suitable for use in recognition software. Information on the generation of the iris recognition codes and the statistical theory used to determine identification of persons was examined.

A single individual provides the basis for the technology used for converting the iris images into a unique code. Dr. John Daugman, of the University of Cambridge provided technical and research papers on the technology he developed, and provided direct World Wide Web resources for updates to the published information. He also referenced the web resources produced and maintained by IriScan Incorporated for additional technology updates. Dr. Daugman has licensed his technique to IriScan Incorporated. IriScan has the rights to license the technology to other companies and expand the use of iris recognition in the private sector. The data used in determining the properties of the iris codes was provided by British Telecom, who has a database of several million iris codes to use for research. The key items of data primarily involve the size of the resulting iris code, the randomness of the generated iris code, the independence of the iris code, the time required to generate the iris code, and the flexibility in generating the iris code.

Phase Three – Cryptographic Security

Phase three involved the examination of the generated iris code for cryptographic security. This involved examining the recognition code that was generated using Dr. Daugman's encoding methods and determining the effort required in either cracking the code or successfully generating a duplicate of the code. It was also necessary to validate the probability of two irises generating the statistically same code as remote. This portion or the thesis relied heavily on the work of Dr John Daugman who collaborated with the opthamologists to make this code, and the data provided by British Telecom for analysis. This portion uses probabilistic methods to determine the effort required to compromise an iris recognition code.

Phase Four – Smart Card Ability

Phase four was validation that the iris recognition code could be stored on a smart card in a secure manner, preventing compromise of the code should the card become lost or stolen. This involved looking at the storage and processing requirements for iris recognition processing and how any other data on the card could be locked from access using this code. Validating that the biological feature was living was also a requirement to access the smart card.

III. Literature Review

Biological Basis

The first part of the iris recognition technology that must be understood is the biological component upon which it is based. Figure 3-1 shows multiple images of the biological feature of interest, the iris.

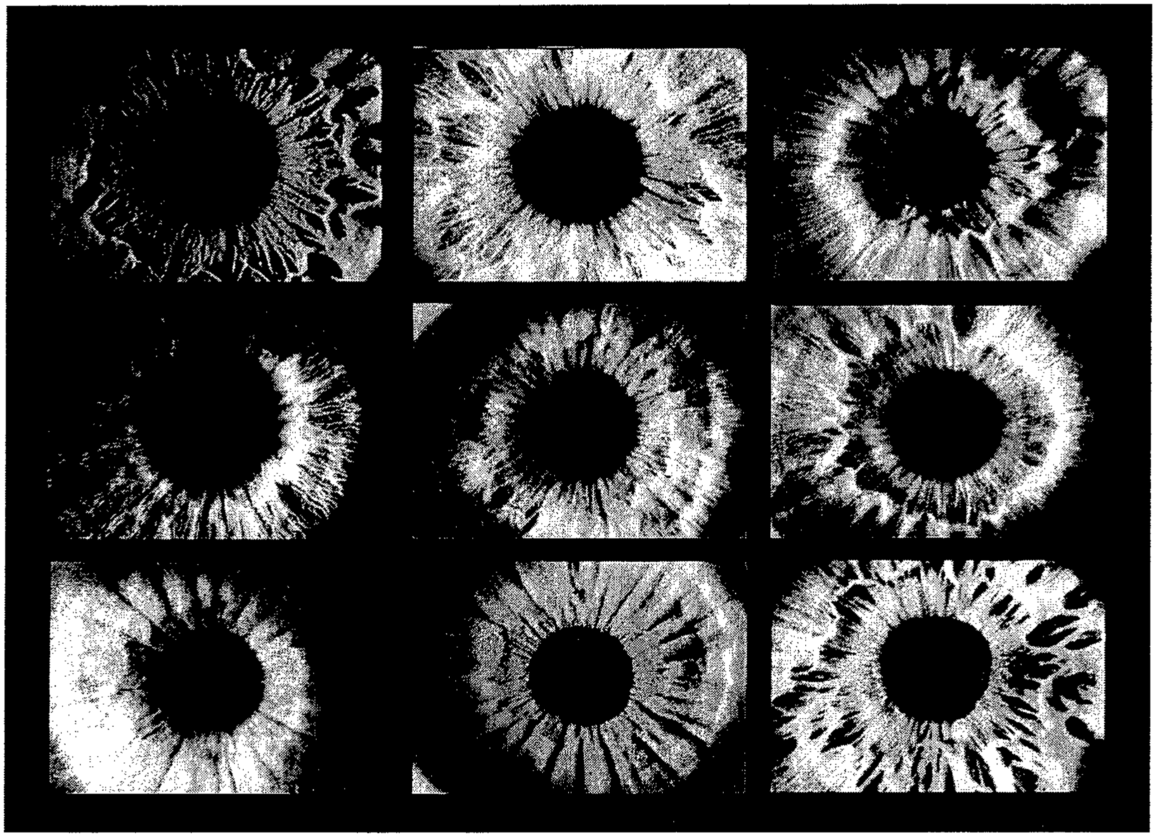


Figure 3-1. Images of Irises (Daugman, 2000)

According to the 2000 Interactive Britannica encyclopedia, the iris is the …

> "…pigmented muscular curtain at the front of the eye, between the cornea and the lens and perforated by an opening called the pupil. The iris consists of two sheets of smooth muscle with contrary actions, expansion and contraction. These muscles control the size of the pupil and thus determine how much light reaches the sensory tissue of the retina. The sphincter pupillae is a circular muscle that constricts the pupil in bright light; the dilator pupillae expands the opening when it contracts. The amount of pigment contained in the iris

> determines eye color. When there is very little pigment, the eye appears blue; with increased pigment, the shade becomes deep brown to black."

The iris is located in the center of the eye, bounded by the pupil and the limbus, just inside the major arterial circle as seen in Figure 3-2. The Iris is internal to the eye and lies between the cornea and the lens of the eye. It is not a flat disk but has a three-dimensional shape, most closely resembling a shallow truncated cone. This shape is due to its position on the lens of the eye that has a convex shape. It is not symmetric as the pupil is located slightly nasal to the center of the cornea. It is surrounded by the aqueous humour and appears to be enlarged by approximately an eighth of its true size when viewed from the front. The aqueous humour is the watery, alkaline liquid that occupies the chambers of the eye--the space in front of the iris and lens and the ring-like space encircling the lens. The aqueous humour is like blood plasma in composition, but contains much less protein, less glucose, more lactic acid, and much more ascorbic acid. Aqueous humour is made from the blood by filtration through the surface of the back of the iris and of the muscular structure that controls the curvature of the lens. It leaves the eye through a porous tissue into a ring-like passageway around the outer angle of the front chamber. From the passageway, the liquid enters the veins (Webster, 1996; Britannica, 2000). The iris changes in thickness and shape depending on its state of contraction. It is short and thick when contracted, and thin and flat when not contracted. The center edge of the iris is round where it borders on the pupil (Loewenfeld, 1993; Alexandridis, 1985).

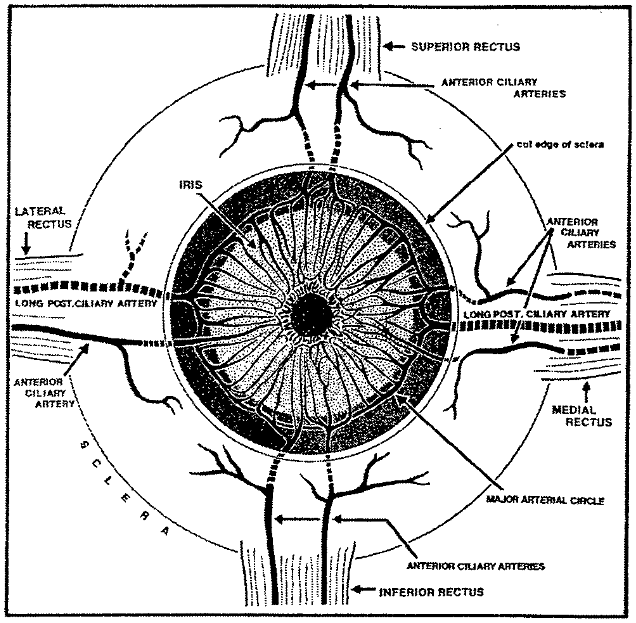


Figure 3-2. Iris from in Front (Loewenfeld, 1993)

The main function of the iris is to regulate the amount of light that is allowed to reach the retina by adjusting the size of the pupil. The iris varies in size from fully relaxed to fully constricted. When fully constricted, it is approximately 13% of its normal relaxed length. The retina initiates this action as the amount of light it receives varies (Alexandridis, 1985).

It was long thought that the movements of the iris was controlled by vascular pressure, but according to recent understanding of anatomic and physiologic evidence, all iris movements are controlled by the iris muscles alone. The movements of the iris muscles carry other structures in the iris passively. These other structures may influence the movements some by their bulk, inertia, and flexibility, but they do not play an active role. These movements follow a linear range of dilation and contraction. At each end of the range, the response of the iris muscles changes as the extremes are reached (Loewenfeld, 1993).

Figure 3-3 and Figure 3-4 show the structure of the iris. The Dilator pupillae, which extends radially thorough the iris, and the Sphincter pupillae, a ring of fibers in the iris, are responsible for the movement of the iris. The ophthalmic artery provides the blood flow to the iris, the major arterial circle supplying a portion of the blood to various parts of the iris. Crypts are formed from the stromal collagen network that supports the structures of the iris (Loewenfeld, 1993).

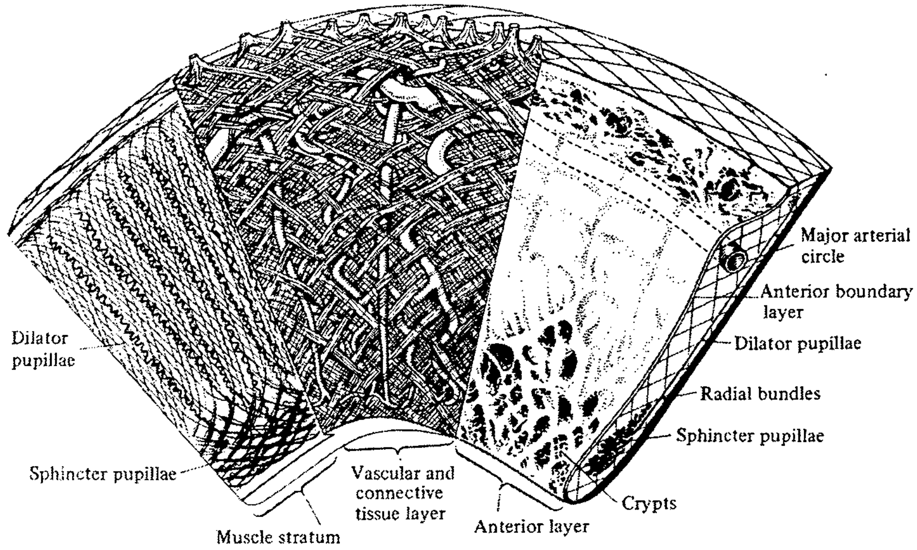


Figure 3-3. Structure of the Iris (Alexandridis, 1985)

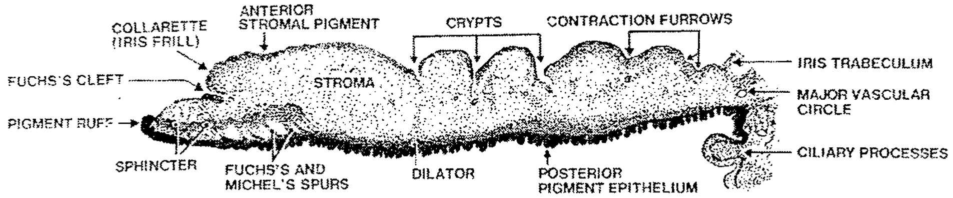


Figure 3-4. Cross-section of human iris in mid-dilation (Loewenfeld,1993)

The general type and color of the iris structure is determined genetically. It has been known for many centuries to run in families. In man, brown eyes are dominant and pale ones recessive. Therefore a blue-eyed and homozygous brown-eyed parent will have brown-eyed children. The eyes of Monozygotic twins, twins resulting from fertilization of one egg by one sperm followed a division early in development, are remarkably alike, not only in childhood and adult life but even in the timing and kind of aging changes that develop. Details of iris structure vary, however, in their degree of genetic congruence as shown in Table 3-1. The eyes of dizygotic twins, twins resulting from two distinct fertilizations and as different as two ordinary siblings, do not seem to have as much genetic similarity (Loewenfeld, 1993).

Table 3-1. Similarity of Iris Details among Twins (Loewenfeld, 1993)

Traits	Complete Congruence in	
	Monozygotic twins (73 pairs)	Dizygotic twins (70 pairs)
Iris Color	72	25
Structure of the pupil edge	70	17
Outline & position of collarette	65	11
Pigmentation (exclusive of naevi)	70	13
Naevi	21	13
Number, size & position of crypts	40	4
Number, size & depth of radial folds	50	8
Number and completeness of contraction furrows	54	14
Density of vessels	66	19
Height of vessels (stromal thickness)	68	39
Vascular course	68	16

The iris forms from the rim of the primitive optic cup that begins to bud forward during the third month of embryonic life (Loewenfeld, 1993). The iris stabilizes during the eighth month of gestation and remains stable throughout a person's lifetime, with the exception of some pigmentation that changes the color of the iris but not the structure (Adler, 1965).

Iris Recognition Technology

In order to have a viable biometric system, there must be a good basis on which to build the technology. There are many different physical or physiological biometrics available. For instance, the following biometrics are available:

Table 3-2. Description of Various Biometrics (Buda, 1999)

Biometric	Definition
Body Odor	A physical biometric that analyzes the unique chemical pattern made up by human body smell.
DNA	A unique, measurable human characteristic.
Ear Shape	A physical biometric that is characterized by the shape of the outer ear, lobes, and bone structure.
Face Recognition	A physical biometric that analyzes facial features, including the shape of the head or face or thermal patterns.
Finger Geometry	A physical biometric that analyzes the shape and dimensions of one or more fingers.
Finger Image/Fingerprint	A physical biometric that analyzes at the patterns found in the tip of the finger.
Hand Geometry/Recognition	A physical biometric that involves analyzing and measuring the shape of the hand.
Iris Recognition	A physical biometric that analyzes iris features found in the colored ring of tissue that surrounds the pupil.
Keystroke Dynamics	A behavioral biometric that analyzes typing rhythm when an end user types onto a keyboard.
Palm Analysis	A physical biometric that analyzes the palm of the hand. Typically, this will involve an analysis of minutiae data.
Retinal Scan	A physical biometric that analyzes the layer of blood vessels situated at the back of the eye.
Signature Verification	A behavioral biometric that analyzes the way an end user signs his/her name. The signing features such as speed, velocity, and pressure exerted by a hand that is holding a pen are as important as the static shape of the finished signature.
Speaker Verification	A part physical, part behavioral biometric that analyzes speech patterns. Some implementations of this technology can separate overlapping voices from each other and other background noises. Other implementations may or may not depend on the user saying a fixed set of numbers or words.
Vascular Patterns	A physical biometric under development that analyzes the pattern of veins in the back of the hand.

Of these, iris recognition appears to be the most secure biometric identification technology based on the number of unique random characteristics that each biometric has available for encoding. The basis for iris recognition comes from the scientific community. It must be considered that there are people that sound alike, look alike, and even have the same DNA. Identical twins and injuries all cause problems for biometric identification systems. Each of these problems has to be addressed and the impact of each must be considered and overcome in a usable fashion (Daugman, 1998; IriScan, 2000). Iris recognition addresses these problems.

While some biometric systems have only a few identifying characteristics, iris recognition has over 400 different identifying characteristics, but only approximately 266 are used in the encoding processes discussed here (Daugman, 1998). Fingerprint identification, which is widely used for positive identification, has approximately 35 distinguishing characteristics. Face identification systems use 64 characteristics (Denning, 1999). Iris recognition therefore contains many more characteristics that are useful to identify an individual uniquely.

Identical twins can cause other problems. Trying to separate identical twins using physical characteristics such as the face is a great challenge considering how much identical twins resemble each other. These types of commonality are referred to as either genotypic or phenotypic features. Genotype is a genetic shared constitution. Phenotype is the actual expression of a feature, affected by the genotype, environment, and the development of that feature. Genotypic features include blood group and DNA sequence. Phenotypic features include fingerprints, face prints, and iris patterns (Daugman, 1998).

Genetically identical people share all their genotypic features. These features are genetic items such as gender, blood group and DNA sequence. All biological characteristics of people can be placed at various points along a genotypic-phenotypic continuum. Some features are solidly on either end of this spectrum while others fall along the continuum. The type of features used becomes very important as phenotypic features may or may not change over time. Genotypic features are static in nature. The properties of these biometric features directly influence the basic error rates. Identical twins, people who share all genotypic features, cause the basic False Match rate, which is called the genotypic error rate. The error rate is approximately 0.82% due to the natural birth rate of identical twins. The minimum rate of False Rejections, called the phenotypic error rate, is created by the tendency of some features to change over time. The goal of a biometric is to minimize or eliminate both the False Match Rate and the False Reject Rate. The link between these two rates and the corresponding biometric features is shown in table 2-3 (Daugman, 1998).

Table 3-3. Performance Limitations based on Feature (Daugman, 1998)

Type of Feature	Performance Limitation
Genotypic	False Match Rate ≥ birth rate of identical twins
Phenotypic	False Reject Rate ≥ feature variability over time

As indicated earlier, the iris, composed of elastic connective tissue, begins to form at the end of the first trimester of pregnancy and is completely formed before birth. The iris pattern does not change during the lifetime of the individual. Since the iris is an internal organ, it is not subject to the same factors of deformation to which other parts of the body are subject. It is immune to the environment except for its reaction to light. In addition, the left and right irises on a single person are entirely uncorrelated. This means that the combination of two unique iris patterns would be unique. This type of uniqueness may become even more important should cloning ever come into use since clones would have the exact same DNA but different iris patterns (Daugman, 1998, 2000; IriScan, 2000).

The remaining challenge for a good biometric identification process is to develop a method to measure, encode and store the data so that it is useful for identification measures. Dr John Daugman developed a process to do exactly that in 1994 and his technique is the basis of all use of iris recognition by IriScan, the major developer of iris recognition technology (IriScan, 2000).

The Iris Recognition Process. A usable biometric identifier has many primary features. It must be able to be encoded quickly and accurately. It must also be extremely varied across the population as a whole (IriScan, 2000). The iris has the good variation, and the technique developed by Dr Daugman provides the statistical encoding method that is both quick and accurate.

Dr. Daugman's technique is based on the scientific evidence that the iris does not change over time. The random patterns of each iris represent a unique code that can be used as an identification feature. The iris, by its nature, is stable and protected, making it very useful for identification during the entire lifetime of the subject. This is an immense advantage over other biometric measures that do not have these features (IriScan, 2000).

The process of iris recognition begins with the imaging of the iris using a video camera and the digital processing of the image to locate the measurable characteristics of the iris. A specialized camera, that passively illuminates the eye with non-visible light, does the imaging process. The processing takes into account light, eyelid location, and photo quality that may vary from photo to photo. This variation is part of what makes iris recognition secure since the changes that are constantly occurring can be detected and must exist for the iris to be living. Even in constant lighting conditions, the iris moves minutely. Once the image is taken, the first requirement in processing the image is to find the inner and outer boundaries of the iris precisely (Daugman, 1993, 1998; Shannon, 2000).

The method used to process the image data is a complex mathematical process that generates unique codes for every pattern. This mathematical process involves the use of complex-valued 2D Gabor wavelets, Figure 3-5. The size of the iris, due to ambient light, and the distance from the video camera are not factors in this method. The transformation of the image using these wavelets results in a dimensionless coordinate system that is pseudo-polar and maintains consistent points of reference. The dilation and constriction of the iris are easy to reverse mathematically. Currently, recognition of a particular iris can be made from up to three feet (Daugman, 1998, 2000; IriScan, 2000).

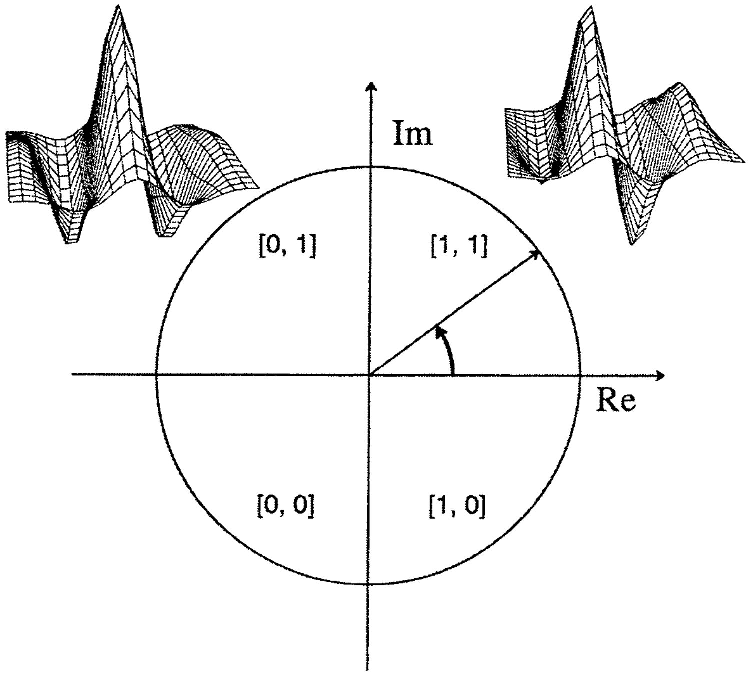


Figure 3-5. Pattern Encoding by phase demodulation using complex-valued 2D wavelets (Daugman, 1998)

Generation of the 256-byte "IrisCode" is accomplished by demodulating it with 2D Gabor wavelets. Figure 3-6 shows the isolation of the iris and the resulting iris code (Daugman, 1993, 1998).

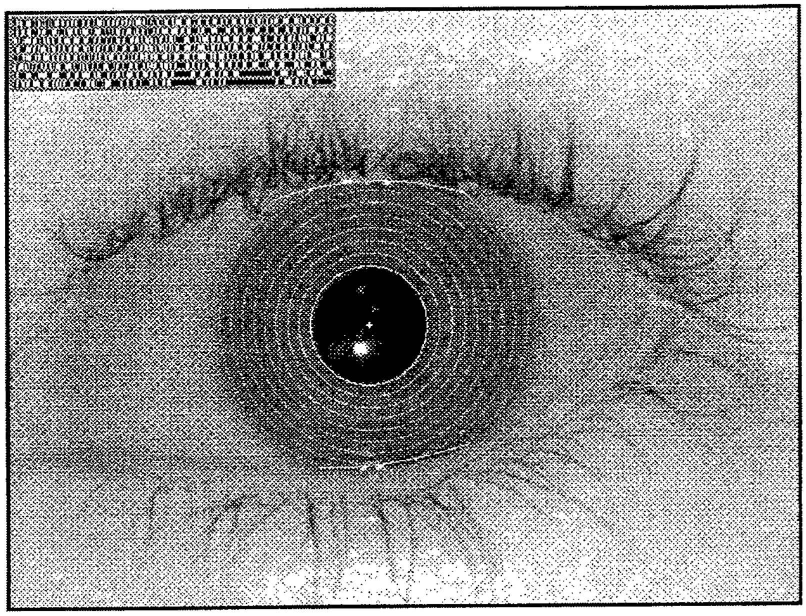


Figure 3-6. Isolation of an iris for encoding, and its resulting "IrisCode" (Daugman, 1998)

The pseudo-polar coordinate system compensates automatically for the stretching of the iris tissue as the pupil changes in size. The encoding process takes place as the texture of the iris is demodulated over very small measurable distances. This encoding process allows for effective translation of images of the iris from behind corrective lenses, such as contacts and glasses. The distortions caused by corrective lenses are mathematically corrected for by the process (Daugman, 1998).

Mathematically, this process of encoding the texture of the iris into a digital code is described as follows:

> … local phase quantization is described by the following conditional integral equations, in which each code bit *h* is represented as having both a "real part" h_{Re} and an "imaginary part" h_{Im}, with $h = h_{Re} + ih_{Im}$, and the raw image data is given in a pseudo-polar coordinate system $I(\rho,\phi)$:

$$h_{Re} = 1 \text{ if } \mathrm{Re} \int_\rho \int_\phi e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi \geq 0$$

$$h_{Re} = 0 \text{ if } \mathrm{Re} \int_\rho \int_\phi e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi < 0$$

$$h_{Im} = 1 \text{ if } \mathrm{Im} \int_\rho \int_\phi e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi \geq 0$$

$$h_{Im} = 0 \text{ if } \mathrm{Im} \int_\rho \int_\phi e^{-i\omega(\theta_0-\phi)} e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} I(\rho,\phi)\rho d\rho d\phi < 0$$

(Daugman, 1993, 1998)

The specifics of these equations are beyond the scope of this thesis. These are complex integral equations used to convert the raw image into a 256-byte digital code (Daugman, 1998, 2000). This code is then used as the basis for comparison in authentication tests. The uniqueness of this code is vitally important to the security of the system. Independent variations and large variety in generated iris codes are critical to the success of this system. Figure 3-7 shows the probability of each bit in an iris code being set in a sample of 222,743 different pairings of IrisCodes compiled by British Telecom. 128 bits were chosen randomly from all parts of the iris code in this figure. The flat curve and the probability hovering around 0.5 indicate that each bit is equally likely to be set or cleared when comparing independent iris codes (Daugman, 1998, 2000).

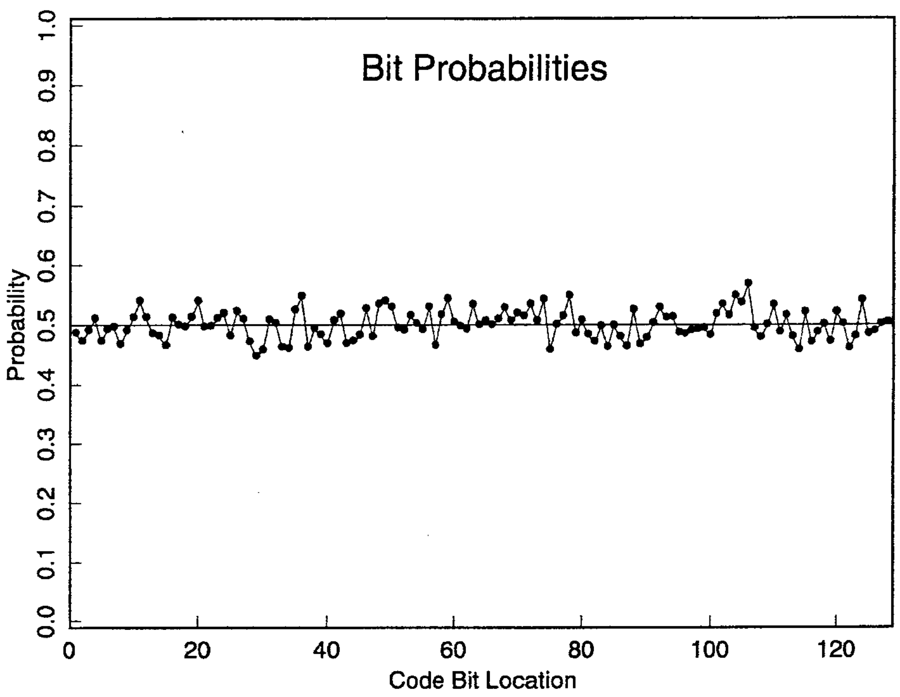


Figure 3-7. Test for Independence of Code bits across a population of IrisCodes (Daugman, 1993)

Figure 3-8 shows the comparison of 2.3 million iris code pairings. This figure shows a histogram of the Hamming distances in those pairings. Hamming distance is the sum of the linear differences between individual symbols between two strings. The Hamming distances here are determined by vector exclusive OR'ing to determine the fraction of the bits that disagree between independent iris codes. This diagram shows that the number of bits of disagreement between pairings runs predominantly between 0.47 and 0.53. This means that two IrisCodes will generally differ by approximately 50% of their bits. A curve fitting this histogram is a binomial distribution with 244 degrees-of-freedom. This data indicates that although the bits are equally probable of being set between independent iris codes, there is a significant correlation of the bits within a single iris code, leaving you with 244 statistically independent bits of the 2,048 bits in an iris code. These bits are different between iris codes and are not common between any code. As a result, the number of statistically independent bits is not useful in trying to fake the code. With minimum values of 0.353, one can set a threshold of less than 35% mismatch and be highly confident of a person's identity (Daugman, 1993, 2000, 2001; Gruska, 1997).

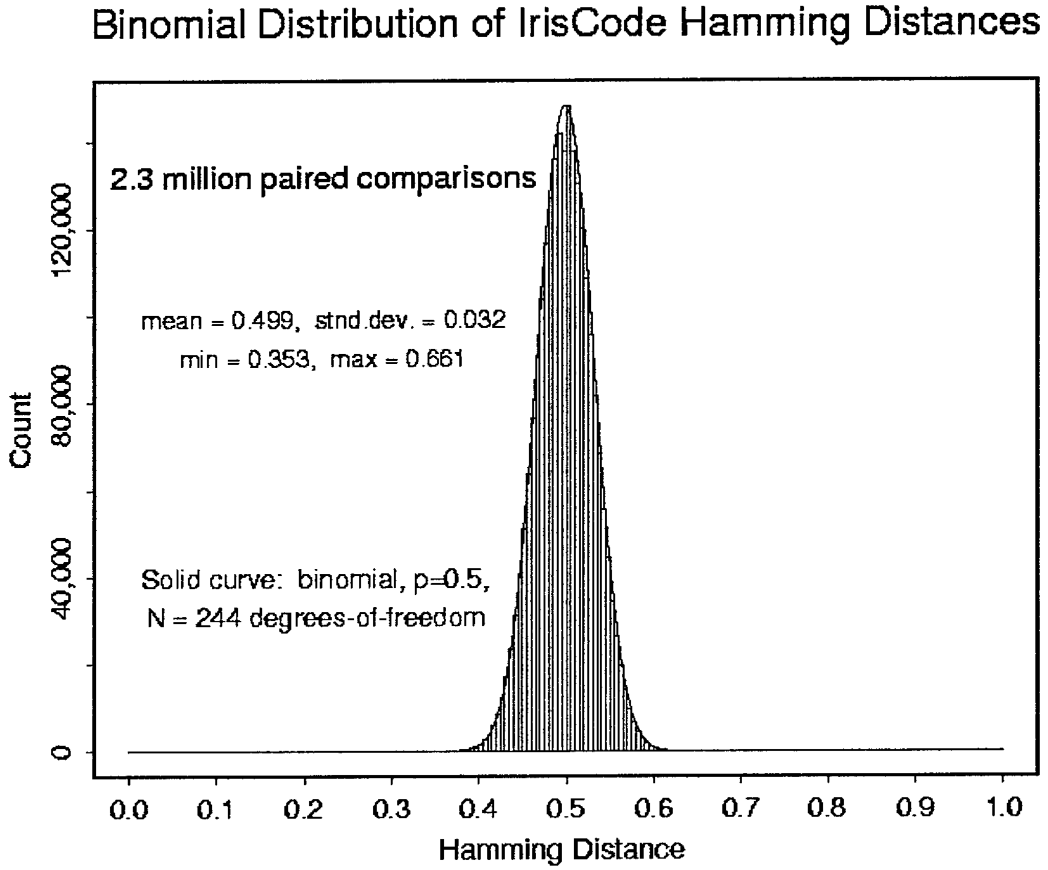


Figure 3-8. Hamming Distances of unrelated IrisCodes (Daugman, 2000)

The other factor that must be considered is those people who are genetically identical. It must be determined if that will cause a problem for this system. Figure 3-9 shows a histogram of the Hamming distances on 648 eyes as 324 Right/Left pairings. As can be seen, the results have a shape very much like the genetically different irises compared earlier. This demonstrates that a person's eyes each have a unique iris pattern. This effectively eliminates the problem of any type of twins causing invalid false accepts in the identification system (Daugman, 1998).

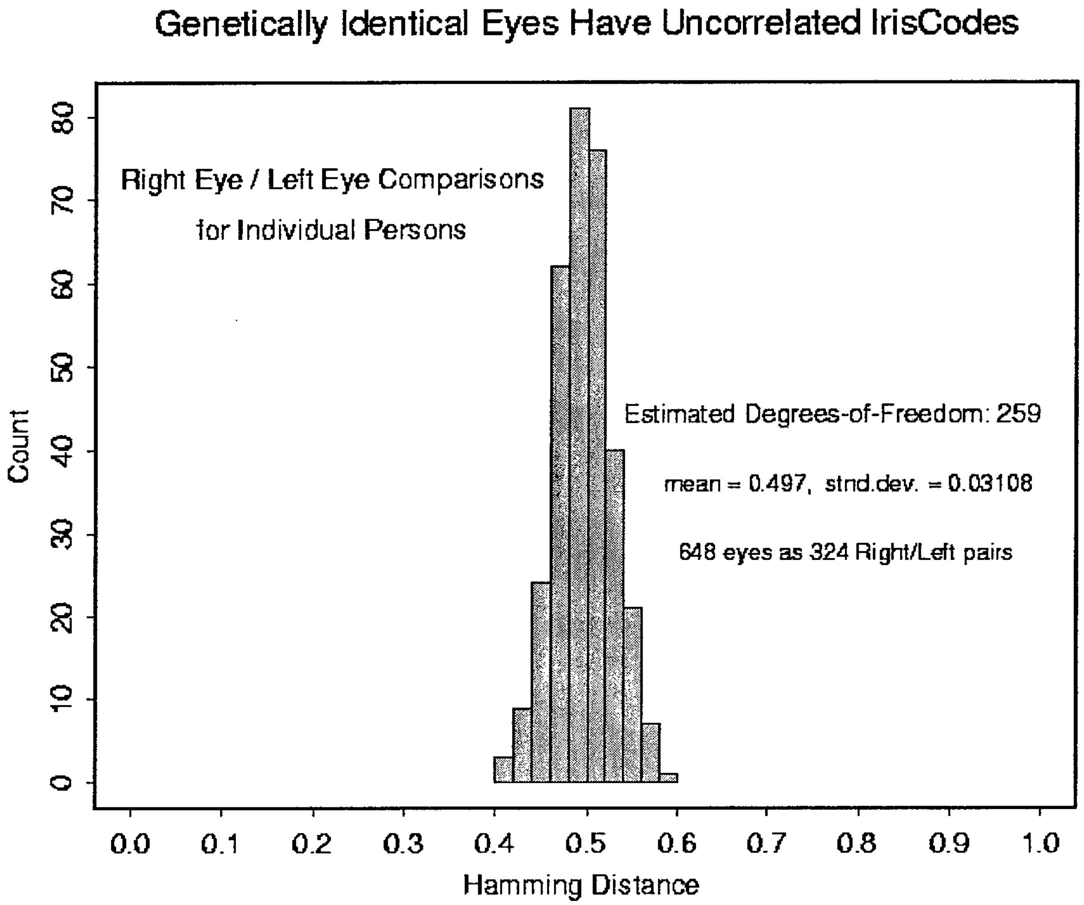


Figure 3-9. Hamming Distances between IrisCodes of Genetically Identical irises (Daugman, 1993)

Using this IrisCode for identification raises the question of how do the Hamming distances between authentic users and impostors compare. Due to the variability of light, distance, eyelid location, pupil dilation and image quality, the IrisCode generated on the spot for comparison is generally not identical to the one generated for enrollment. As shown in Figure 3-10, there is some variation in the number of bits that differ, and there are almost always differences in the authentic user. However, the figure shows that the differences for impostors are significantly different from the differences for authentics. Since there is a sizable area between the two sets of codes, a tolerance can be set between them and one can be confident of high reliability in identification (Daugman, 1998).

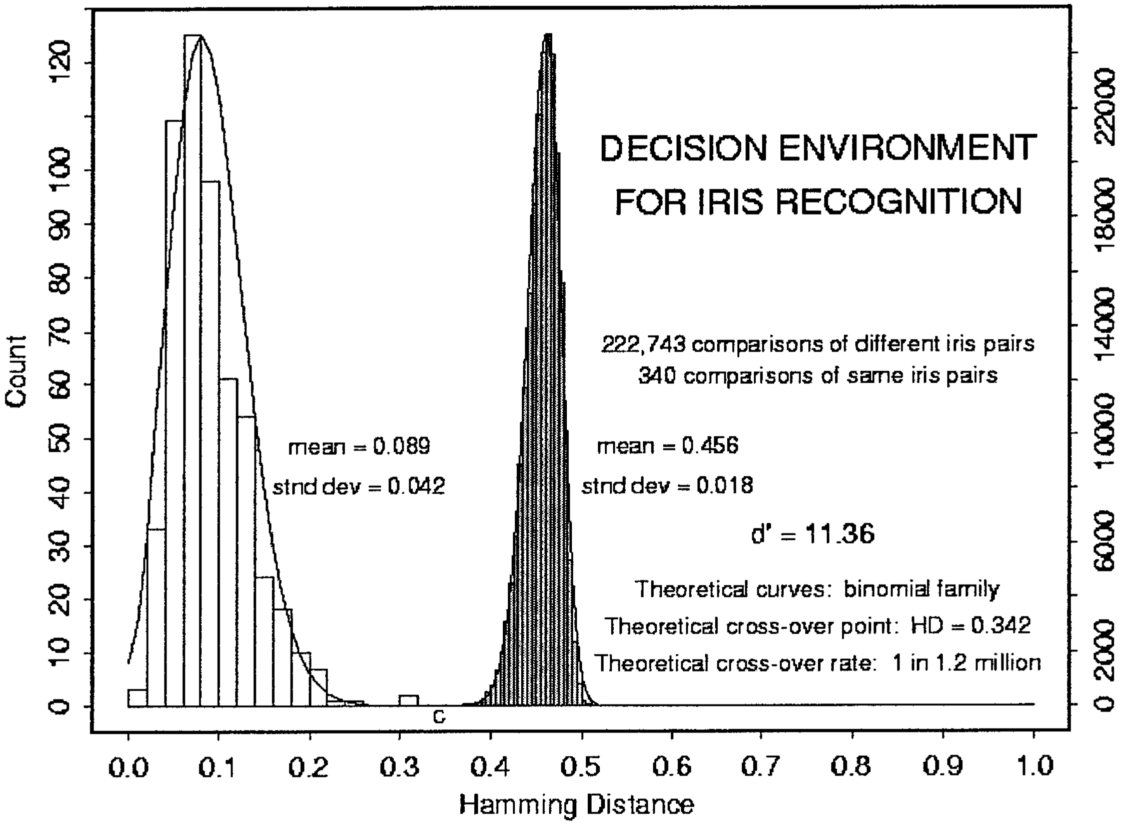
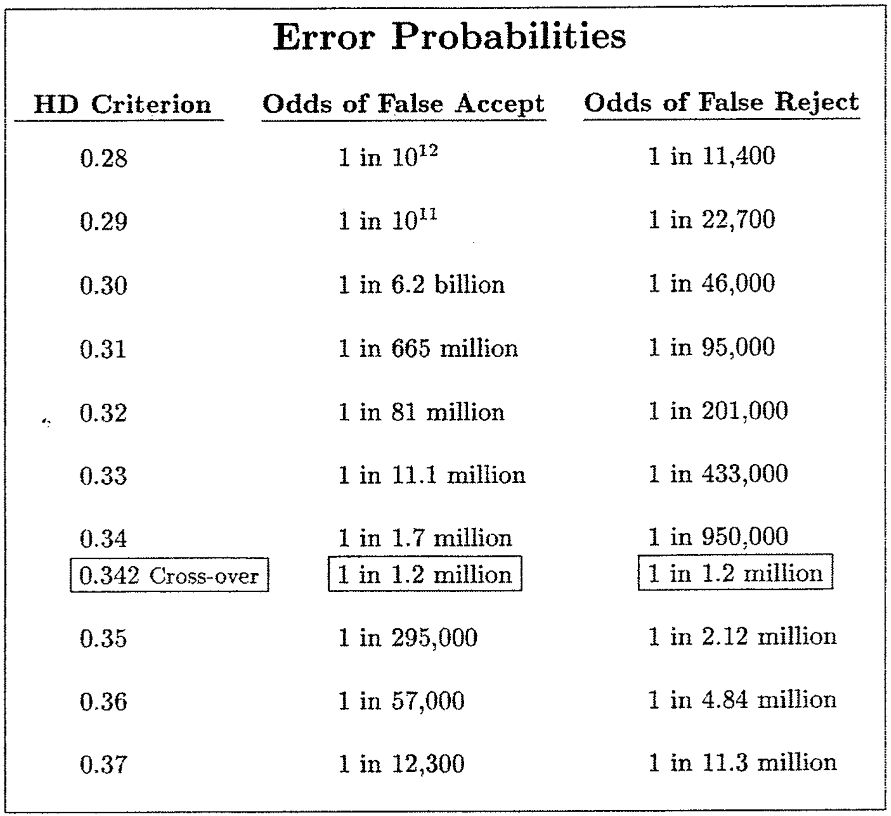


Figure 3-10. Decision Environment For Identification Using Iris Patterns (Daugman, 1993)

For access to a system, an image is captured by a specialized camera and passed to a computer for analysis. The IrisCode generated by the computer is then compared to the database of authorized users. The algorithm used tests to see if the new code is statistically independent of the codes in the database. If it fails the test for independence, the user is authorized access. Impostors will always generate statistically independent IrisCodes where authentics will not. This test for independence can be trimmed based on how much error is considered allowable. Theoretical error rates for various hamming distances have been computed based on the data from British Telecom. The error probabilities are shown Table 3-4. The crossover rate, which is the location where the error probabilities cross each other is approximately 0.342. This means that in excess 1/3 of the bits can differ while still getting a valid identification of a person. Even with 1/3 of the bits disagreeing, the odds of two irises generating a sufficiently common code are estimated at 1 in 1.2 million codes as shown in Table 3-4 (Daugman, 2000).

Table 3-4. Error Probabilities (Daugman, 1998)



Error Probabilities

HD Criterion	Odds of False Accept	Odds of False Reject
0.28	1 in 10^{12}	1 in 11,400
0.29	1 in 10^{11}	1 in 22,700
0.30	1 in 6.2 billion	1 in 46,000
0.31	1 in 665 million	1 in 95,000
0.32	1 in 81 million	1 in 201,000
0.33	1 in 11.1 million	1 in 433,000
0.34	1 in 1.7 million	1 in 950,000
0.342 Cross-over	1 in 1.2 million	1 in 1.2 million
0.35	1 in 295,000	1 in 2.12 million
0.36	1 in 57,000	1 in 4.84 million
0.37	1 in 12,300	1 in 11.3 million

The theory behind this decision-making is called Statistical Decision Theory. It is based on Yes/No recognition decisions having four possible answers, two valid and two invalid. The two valid decisions are acceptance of a valid user and rejection of an invalid user. The invalid decisions are acceptance of an invalid user and rejection of a valid user. This decision theory is represented in Figure 3-11. It shows how the four decisions interact with each other. There are some decisions that overlap in the diagram indicating where errors in decisions may occur. (Please note that the decision curves shown in Figure 3-11 are generic and not based on the iris recognition technology) (Daugman, 1993).

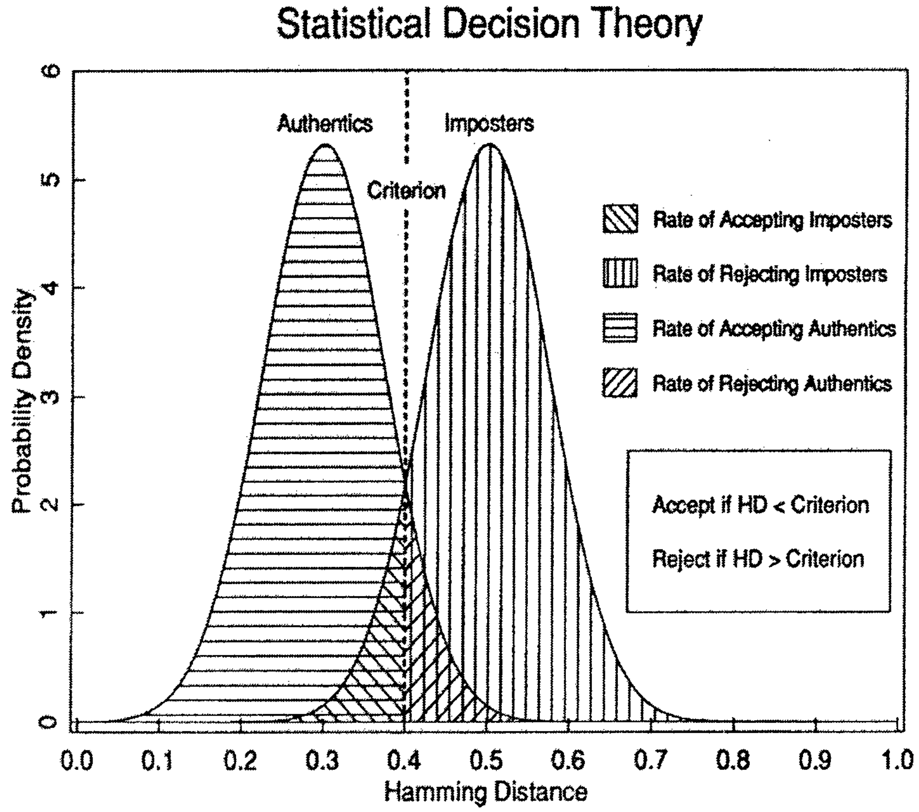


Figure 3-11. Statistical Decision Theory (Daugman, 1993)

Figure 3-12 provides guidance on how strict to set the decision making and the effects it has on the authentic and impostor acceptance rates. The more conservative the decision must be, the fewer impostors that are accepted and the more liberal the decision, the more impostors that are allowed. It is up to management to make the decision on how strict the decision must be for the level of security that they require.

Figure 3-10 gives a much closer example of how the iris codes fall in the same system and the best location for a criterion cutoff is in the region between the curves (Daugman, 1993).

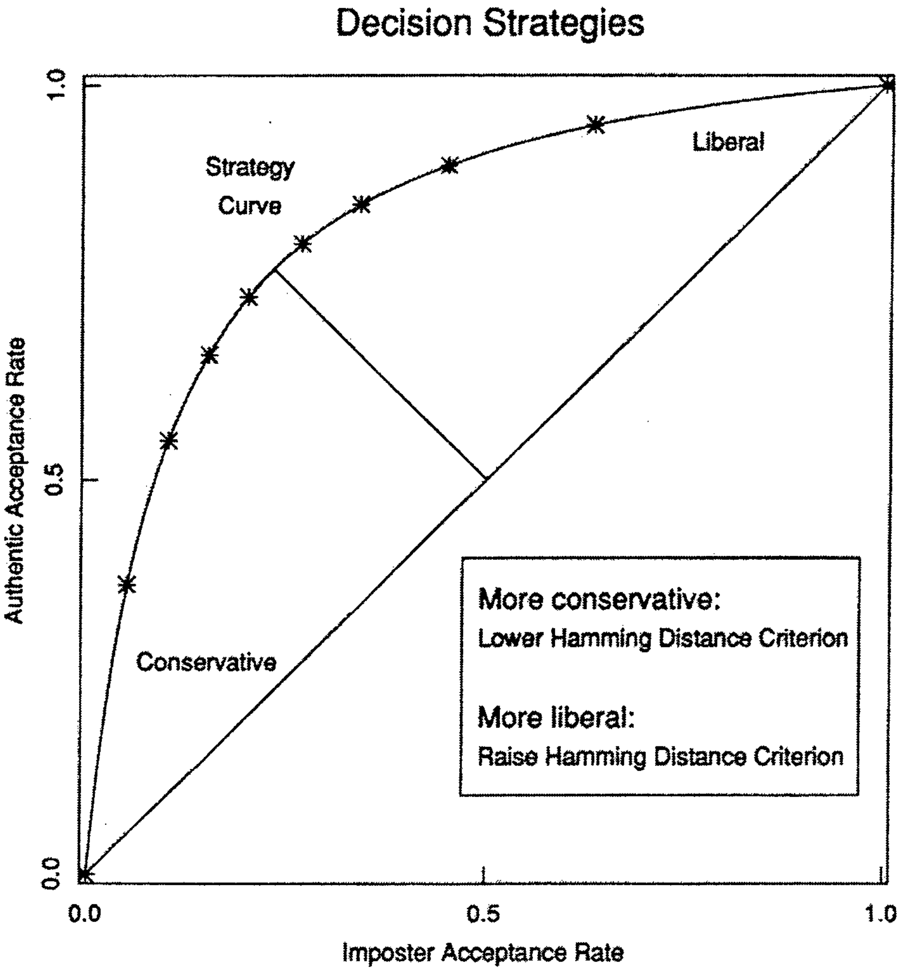


Figure 3-12. Neyman-Pearson Decision Curve (Daugman, 1993)

Once management has decided on the decision threshold, the recognition system can be installed and implemented with confidence. Once the code is generated and compared to the database, action is taken based on the outcome. It either allows access or denies access. After access has been determined, the iris recognition process is concluded.

Safety of Iris Recognition. Safety of an identification system is exceptionally important. In order for a system to gain wide acceptance, the using population must be assured that the technology used will not harm it. Much of the safety involved is communicated to the users of the system by the way it is used. Iris recognition does not require contact with the subject, although the distance over which the identification is viable is currently short range. However, within a range of about three feet, the recognition process is very quick and accurate. Most eye surgeries, contacts, masks, and glasses do not interfere with the recognition system and make it even more versatile. Even the American Academy of Ophthalmology has examined the technology and publicly stated that it is perfectly safe. There are other systems that use the eye as part of the identification process that are not nearly as safe, such as intrusive infrared or ultraviolet technologies. The current iris recognition system uses a passive non-visible light to illuminate the iris for imaging; it is not intrusive in nature (Diebold, 2000; Shannon, 2000; Daugman, 2000).

Counterfeit Detection. Counterfeit access is another problem. For the purposes of a biometric, it must be determined if the biological feature is still living and attached to the authorized person. The iris makes this very easy. The iris is in constant motion even under steady illumination. It oscillates at about 0.5 Hz. In addition, it reacts very quickly to changes in lighting conditions. The camera that is imaging the iris can detect this motion. If the motion is not detected, then it must be a fake and will not be recognized. In addition to this motion, light reflects differently from a living eye than from a photo or other reproduction. This can also be detected by the images being sent from the camera. Images that are not internal to the eye have characteristic light refraction patterns that are readily detected (Daugman, 1998).

Advantages and Disadvantages. As with any system, there are many advantages and disadvantages to this technology. Further advancements in technology will sometimes overcome the disadvantages and additional research may discover new ones. Currently, the advantages of iris recognition technology are:

- Internal organ not exposed to outside elements directly
- Can be seen from a distance
- Can be viewed even through corrective lenses
- Every iris is unique, even in identical twins
- Natural movement of the iris is predictable and useful in detecting fakes
- Early development and no significant change over the subjects lifetime
- Good statistical method to map and encode the iris pattern
- Speed of recognition is very fast, processing requires less than 1 second
- Recognition hardware is unobtrusive
- Much of the needed equipment is inexpensive and readily available
- Easy for anyone to use since user intervention is not required

The disadvantages are:

- Small object which makes it difficult to get a good image at a distance
- Moving target
- "Big Brother" syndrome when public is uneasy over passive surveillance
- Compromise of the identity codes can make entire system useless
- Located behind the cornea which is a curved, reflective surface and usually moist
- Eyelashes, reflections may obscure it
- Eyelids my occlude the iris
- Iris deforms non-elastically as pupil changes in size
- Illumination of the iris needs to be non-visible and of low intensity

(Daugman, 2000; British Telecom, 2000).

Existing Uses of the Technology. This technology is not just theory. Several initiatives are currently underway that use iris recognition technology. The United States Army is working on methods to eliminate passwords on their systems. The Army has very specific and restrictive missions that make voice and fingerprint technologies less useful than other biometric systems. Army personnel must be able to work in protective gear and in hostile environments (Daukantas, 1999). For example, gas masks and protective suits effectively isolate the individual from the environment making any biometric that requires physical contact impossible. Even biometrics that can be used at a distance, such as voice, are muffled and do not provide a clean identification token. The iris recognition system, however, can be used through the clear face shield on protective suits and provide a viable means of identification. Iris recognition also works through corrective lenses providing usability through any gas mask or glasses.

Banks have already started to integrate this new technology into existing systems. In the last six months of 1998, the Nationwide Building Society located in England started using ATM machines that used the iris recognition technology to identify clients and provide services. Their implementation was successful and the customers had very high confidence in the new technology (Sensar, 2000). In May 2000, Bank United brought the technology to the US banking industry. In November 2000, the Houston, Texas, bank became the forerunner and installed an ATM machine that implemented the iris recognition technology to identify its customers like the Nationwide Building Society did in England (Diebold, 1999; USA Today, 1999). These new ATM machines may eliminate the tokens that everyone is accustomed to using to access their accounts. The United States is just starting to work with the technology, but there are 11 banks outside the United States that have already implemented this technology. This type of technology may eventually find itself applied in other types of financial transactions as well (USA Today, 1999).

A system to control access to individual computer systems has been developed by British Technology Laboratories. They have engineered software to control access to Windows NT computers, networking systems to share a common identity database, and securing smart cards (Gifford, 1999). All of these demonstration systems have applications in the military environment. They could eliminate passwords used to access computer systems and make smart cards, like the Fortezza card, more secure by making it work only when the user is verified by an iris scan. That would prevent unauthorized access by other parties should the card become lost or stolen.

This technology will even work for blind people to a great degree. Many of the causes of blindness do not affect the iris. Identification using iris recognition is usable in all cases where the iris is not involved in the degenerative condition causing blindness. Only in cases where the condition causes a degeneration of the iris or occlusion of the iris due to clouding of the cornea will iris recognition be infeasible for the blind.

Other applications for iris recognition technology abound. It could be used with credit-cards, passports, driver's licenses, anti-theft devices, building access or anything else that currently requires some sort of token for access validation (Daugman, 2000).

Cryptographic Security

For cryptographic testing, key management and generation were chosen as the applicable model since the generated code is what must be kept secure. The iris recognition technology generates a 256-byte key that identifies a person. This key can be mismatched by a certain percentage and still be valid. Figure 3-7 shows that the probability of certain bits being set in any particular iris code is in the 50 percent range indicating randomness in the bits. This means that if the IrisCode is used solely by itself, and not padded with other information, a 256-byte (2,048 bit) random key exists. Table 2-5 shows the equivalent key lengths at various sensitivity levels for a raw IrisCode. This table illustrates the equivalent key size, number of possible variations in that key if used for encryption, and the estimated length of time to perform an exhaustive search for an exact match. If, for the foreseeable future, we follow Moore's Law, which states that computer power continues to double about every 18 months, computing power will still not develop enough to reduce the exceptionally long time required to discover an exact match by exhaustive search (Denning, 1999). All of the figures provided show lengths of time greater than the number of particles in the known universe, by several orders of magnitude. With key lengths of such magnitudes and exhaustive search times of such length, the brute force method of key discovery is infeasible (Daugman, 2000; Schneier, 1996; Denning, 1999).

Table 3-5. Key size and number of variations

Mismatch	Bit length	Variations	Exhaustive Search*
22%	1,597	5.6×10^{480}	2.0×10^{459}
26%	1,515	1.1×10^{456}	3.9×10^{434}
30%	1,433	2.4×10^{431}	8.4×10^{409}
34%	1,351	4.9×10^{406}	1.7×10^{385}

* in millenniums, based on 90 billion attempts per second (July 1998 Maximum Rate on Public code-breaking contest)

The strength of the IrisCode in brute force attempts has been examined, but those are not necessarily the most effective. Other traditional attacks, such as dictionary attacks, do not apply since the code does not use word-based keys. The strongest keys are always considered those based on truly random values. The development of the iris is a random physiological process and therefore the resulting code maintains this property (Daugman, 1998; Schneier, 1996; Schneier, 2000).

Cryptanalysis will be difficult since the code is used as a key for the token and not for encrypting messages. This provides very little additional information to a would-be key breaker to use in his analysis of the key. Most successful cryptanalysis requires quantities of plaintext, ciphertext or both in order to mount a successful attack. The algorithm for encoding the iris could be public since the input to the key generation process is completely random (Schneier, 2000; Daugman, 1998).

Differential Power Analysis has been recently used to monitor the amount of power usage on a smart card to gain information about how long the key is and how difficult is may be. This technique would not be very successful as all iris codes are the same length and the complexity of the code would be very uniform between iris codes. This uniformity would make the power fluctuations uniform between cards and defeat this method of key discovery (Denning, 1999).

Smart Card Implementation

Smart card technology comes in many forms. Figure 3-13 shows an example of a smart card that combines many different functions for the U.S. Government (Holcombe, 2000).

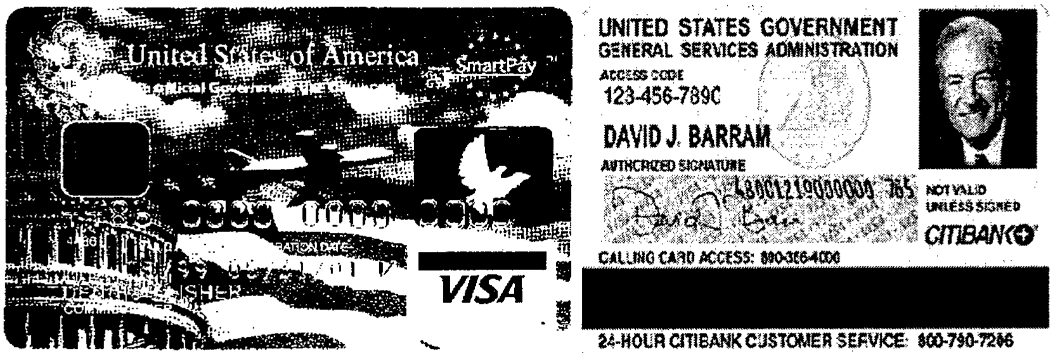


Figure 3-13 - Government Multi-purpose Card (Holcombe, 2000)

This small plastic card can have many uses. It can be used for identification, electronic commerce, fraud protection, digital signatures, and encryption. There are many initiatives in the Federal Government involving smart card technology. The Office of Governmentwide Policy (OGP) has been attempting to identify smart card projects and applications being developed by Federal agencies to make the United States government function more efficiently. Several Air Force smart card initiatives, as registered in the OGP database, are shown below.

Commando Card, Deployment Personnel Accountability Readiness Tool (DPART). The Commando Card is a tailored deployment tool that is being tested in a pilot program with cooperation from the Air Expeditionary Force Battlelab at Mountain Home Air Force Base, Idaho and the Department of Defense Smartcard Technology Office. The cards have been issued to the 16th Special Operations Wing and Hurlburt tenant units involved in the mobility process at Hurlburt Field, Florida. The Commando Card is used to make a large number of programs paperless. The combination of a bar code and chip streamlines the mobility process, easing the creation of manifests, verifying training requirements and medical records and reducing the manual processing associated with the frequent mobilizations at Hurlburt. The card can also store information for used in logistics, security forces and for work center managers.
Technology: Chip, Bar code

U.S. Air Force Identification Card. The U.S. Air Force plans to issue approximately 700,000 new identification cards using smart card technology in December 2000. It has not yet been determined what applications, other that identification, the card will be used for. However the Air Force is studying the use of smart cards for physical and logical access, stored value and record keeping. It is predicted that by mid-2002 all active duty members will have smart cards.
Technology: Chip, Magnetic stripe, Bar code
[NOTE: As of the writing of this thesis, the status of this initiative is not completely known. There has been no indication that it met the December 2000 proposed implementation date.]

United States Air Force Academy Falcon Card. In May of 1998 the Air Force Academy issued to all cadets the first multiple application EMV card to carry independently loaded applications. The cards allow cadets to use the electronic purse to pay for laundry, snack purchases in the laundry areas, and copiers in the library. Additional point of sale locations are being added. Disposable cards in $10 and $20 values can be purchased by USAFA faculty, employees, and family members. The following additional applications have been planned and will be added to the card: student visibility, manifesting, physical access, network access, medical and dental, inventory control, physical and aerobic fitness test results, training qualification, test results and food services. The system was designed to allow the Air Force Academy to continue to add these non-financial applications as well as to be independent yet interoperable with the U.S. Department of Defense Smart Card program.
Technology: 4K contact chip card, Bar code, Photo

Lackland AFB Recruit Card. This pilot launched July 2, 1998, issued Visa Cash cards to recruits arriving for training at Lackland Air Force Base. Recruits are issued a smart card as they arrive that confirms their arrival, completes their registration and disburses $250 as an initial pay advance. The stored value can be used to pay for goods and services at the barber, Post Exchange, dry cleaners, phone center, on-post banks and credit unions and to make donations to the post chaplain. Nations Bank expects to issue approximately 40,000 cards per year to recruits at Lackland Air Force Base.
Technology: Chip, Magnetic stripe

(SmartGov, 2000)

As this list demonstrates, smart card technology is being tried for many different applications. The list is not complete, as there are many other government projects examining smart cards as well as many private sector initiatives that are attempting to take advantage of this relatively new technology.

As shown in the list above, smart card technologies as well as its uses, vary greatly. The technology is rapidly progressing as manufacturers attempt to make the cards hold more information and process more data. The current state-of-the-art smart card uses a 32-bit Reduced-Instruction-Set Computing (RISC) processor, with 32 kilobytes of Electrically Erasable Programmable Read Only Memory (E2PROM), 64 kilobytes of Read-Only Memory (ROM) and 4 kilobytes Random Access Memory (RAM) (Smart Card, 2000). Compared to desktop and laptop computers, this appears to be insufficient to accomplish any work. However, smart cards are used for specialized data storage and processing that does not require the same resources as a desktop computer. The E2PROM is used as the devices permanent storage for data where the RAM is used for temporary storage during processing. The ROM contains the programs the card uses. Some cards also contain a radio transmitter to allow them to be used without physical contact with another device. The E2PROM is designed to retain data for up to 10 years without electrical power and supports a minimum of 10,000 read-write cycles during the life of the card by international standards. Secure smart cards also have a cryptographic engine built in to handle encrypting the contents of the card. The FORTEZZA card, which is used for signature and cryptographic uses has 128 kilobytes of RAM and EEPROM. Configuration of the smart card is highly dependent on what it is designed to be used with. Smart cards are simply very small specialized computers (SmartGov, 2000).

IV. Findings and Conclusions

Conclusion

Each phase of this thesis has addressed a component of the overall question: Can iris recognition technology can be used to secure smart cards? In phase one, the biological basis of the technology was examined to determine if it was stable over time and was unique between individuals.

According to the data collected, the unique development of the iris pattern is a result of multiple layers of tissue forming the iris. These layers of tissue form during the embryonic stage of human development and are in a stable form by birth. This development results in unique iris structures between individuals and between the irises of the same person. There is some change in the color of the iris after birth as the tissues of the eye mature. However, the random pattern the tissue forms during development does not change. In addition to the developmental stability of the iris, its unique position located internally to the eye protects it from environmental factors that could cause a change in the pattern.

Additional data concerned the effects of eye surgery and other corrective measures on the iris pattern. Most eye surgery and other corrective measures used on the eye do not involve the iris, but the cornea. Vision correction, by means of contacts and prescription glasses, distort the image of the iris when viewed from the front. This distortion is in a predictive manner and the technology used accounts for this distortion when encoding and imaging the iris.

In phase two, the technology used to encode the iris was examined. Although the actual implementation details are not examined, the results of the generation of many thousands of iris codes using the selected encoding method showed that the iris code was unique between individuals, reliable in confirming identities of individuals, and extremely difficult to fool. The iris code generated is 256 bytes in length with each bit in the code being equally probable of being set during the generation of the iris code. It is important to note that the IriScan software generates a 512-byte code using the 256 byte Daugman method for its basis. The purpose of these additional bytes is proprietary in nature and not discussed here. The generation of the code takes less than a second on an Intel 486 class computer. The imaging of the iris can be done from a distance of approximately 3 feet with a specialized camera that corrects for variable lighting. The motion of the iris is mathematically determined and accounted for in the calculations. Refractive problems resulting from corrective lenses and the shape of the cornea are also mathematically solved. It uses impostor detection methods to determine that the iris it is examining is alive and not a photograph or glass facsimile.

In phase three, the key strength of the iris recognition code was calculated to be exceptionally strong. The recognition code generated by the Daugman encoding method used by the IriScan software is mathematically generated in such a way that the individual bits of the code are approximately equally probable of being set. This code generation, due to lack of patterns or bit combination restrictions, limits the types of code breaking or generating that can be used to find the code. With all bits being approximately equally probable of being set, the only method of determination currently available is exhaustive key generation. Over the long run, a code breaker would be required, on average, to generate half the possible codes to find the correct one. Due to this requirement, guessing the code is infeasible using any current computer technology. The technology phase shows that the individual irises on a single person are independent of each other and a compromise of the code for one eye would not lead to the compromise of the code for the other eye. Even the compromise of the code is not a large issue since biometric security requires that the presented biological component be living which is exceptionally difficult to duplicate. However, if an unauthorized person is able to get their code into the database of authorized users, the security of the code itself is no longer an issue.

In phase four, current smart card technology was reviewed. The key elements involved with the smart card technology are processing power and storage capacity, taking into account the size of the code to be stored and the necessary programming required to carry out the verification. Other data on the card can be locked from access by encryption. The government Fortezza card already locks information on the card and requires a key to access information. That key is a password that can be replaced by whatever technology is deemed reliable, rapid, and accurate. Smart card technology has sufficient storage and processing power for the application considered here. However, specific implementation details were not examined in this thesis.

In summary, iris recognition technology is a very secure method of making sure only authorized personnel have access to sensitive information. The identification code can be easily stored on a smart card and the processors on the cards can handle the processing required for validation. The code is difficult to break and the technology is easy to use. The data has shown that incorporating iris recognition technology is a viable method of securing smart cards.

Limitations of this research

This research used archival type data with some personal correspondence. Due to the limited history of the technologies examined here, there is little data available beyond what is kept by the vendors for use in producing their products and the original developer of the iris encoding method.

There is a variety of possible implementation schemes for the technologies presented here. No specific implementation schemes were examined to determine the impact on the results of this study.

The cryptographic analysis did not directly examine individual iris recognition codes but relied on the probabilistic statistics provided by the literature. The statistical data does not include direct examination and statistical analysis of the iris codes of twins, but uses opposing eyes in the same individual for analysis of genetically identical iris codes. Direct examination of the iris codes could possibly influence the results of this study.

No cost data was examined to determine if the cost is prohibitive for this usage. The costs involved in setting up the system are difficult to determine without specific implementation details determined.

Suggestions for Further Research

Analysis of the differences between the iris codes of the same eyes on identical twins would serve to determine if they pose a risk to the recognition system. Further research can also be done on different methods of trying to crack a given iris recognition code. The method specified in this thesis was the most obvious method based on the data gathered and no others methods presented themselves as a candidate for use in breaking an iris recognition code.

In addition, a cost analysis would be useful in determining at what point the increased cost of this technology and the cost of compromise of government secrets intersect. Not all government secrets require the best in encrypted protection as the costs for that protection can outweigh the value of the secret under protection.

A detailed analysis of specific smart card implementations of iris recognition technology, comparing the pros and cons of the various implementations would provide options to decision makers should they decide to implement this technology.

Appendix – Email Correspondence

```
Received: from babybear.afit.af.mil (mr-afit.afit.edu [129.92.253.250])
by ms-afit-01.afit.edu with SMTP (Microsoft Exchange Internet Mail
Service Version 5.5.2653.13)
      id DBZBV0ZL; Fri, 19 Jan 2001 11:12:22 -0500
Received: from afit.af.mil ([129.92.253.250]) by babybear.afit.af.mil
          via smtpd (for ds-region10-01.afit.af.mil [129.92.1.5]) with
SMTP; 19 Jan 2001 16:11:48 UT
Received: from wisbech.cl.cam.ac.uk ([128.232.0.15])
 by mr-afit (NAVIEG 2.1 bld 63) with SMTP id M2001011911100221114
 for <orval.phelps@afit.af.mil>; Fri, 19 Jan 2001 11:10:02 -0500
Received: from charybdis.cl.cam.ac.uk
      ([128.232.2.232] helo=cl.cam.ac.uk ident=jgd1000)
      by wisbech.cl.cam.ac.uk with esmtp (Exim 3.092 #1)
      id 14Je7s-00063Q-00; Fri, 19 Jan 2001 16:10:56 +0000
X-Mailer: exmh version 2.0.2+CL 2/24/98
To:     "Capt Phelps,Orval E AFIT/ENV \(E-mail\)"
<orval.phelps@afit.af.mil>
cc: John.Daugman@cl.cam.ac.uk
Subject: Re: Iris Recognition Technology
In-reply-to: Your message of "Fri, 19 Jan 2001 09:59:17 EST."
             <000001c08228$6af7c7a0$0200000a@ophelps>
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Date: Fri, 19 Jan 2001 16:10:48 +0000
From: John Daugman <John.Daugman@cl.cam.ac.uk>
Message-Id: <E14Je7s-00063Q-00@wisbech.cl.cam.ac.uk>

Orval,

   Thank you for your interest and your question:

> I have a question on the Test for Independence of code bits across
> populations of IrisCodes.  According to your papers, there are only
> 244 independent bits in the 2048 bit iris code due to large internal
> correlations in the iris code.  Are these 244 bits the same bits in
> every iris code

    No...

> or are the 244 bits located in different parts of the code for
> each independent iris.

    Yes...

> I am trying to determine if a code breaker could
> simply focus on 244 specific bits in the code or would have to deal
> with the entire 2,048.
>

   To be more precise, there is almost no "single bit" that is
completely independent of all the others.  Rather, the entire ensemble
of 2,048 bits behaves collectively with exactly the same statistics as
```

244 independent Bernoulli trials. This is shown by the following two URLs:

http://www.cl.cam.ac.uk/users/jgd1000/binomdata.html
(compare the theoretical solid curve with the data histogram), and

http://www.cl.cam.ac.uk/users/jgd1000/quanquan.html
(see what a straight line is made by prediction versus observation).

By the way, URL
http://www.cl.cam.ac.uk/users/jgd1000/independence.html shows
independence between bits *FROM DIFFERENT* IrisCodes, not same one.

Best wishes,

John Daugman, Ph.D., O.B.E.
The Computer Laboratory
University of Cambridge
Cambridge CB2 3QG UNITED KINGDOM
tel. +44 1223 334501   fax: +44 1223 334679
Web: http://www.cl.cam.ac.uk/users/jgd1000/

```
Received: from babybear.afit.af.mil (mta1.cl.cam.ac.uk [128.232.0.15])
by mustang.afit.af.mil with SMTP (Microsoft Exchange Internet Mail
Service Version 5.5.2650.21)
      id R8WVTRSS; Wed, 30 Aug 2000 11:56:07 -0400
Received: from mta1.cl.cam.ac.uk ([128.232.0.15]) by
babybear.afit.af.mil
          via smtpd (for mustang.afit.af.mil [129.92.1.107]) with SMTP;
30 Aug 2000 15:56:50 UT
Received: from charybdis.cl.cam.ac.uk
      ([128.232.2.232] helo=cl.cam.ac.uk ident=jgd1000)
      by wisbech.cl.cam.ac.uk with esmtp (Exim 3.092 #1)
      id 13UADd-0006i0-00; Wed, 30 Aug 2000 16:56:05 +0100
X-Mailer: exmh version 2.0.2+CL 2/24/98
To: orval.phelps@afit.af.mil
cc: John.Daugman@cl.cam.ac.uk
Subject: Iris Recognition Technology
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Date: Wed, 30 Aug 2000 16:55:59 +0100
From: John Daugman <John.Daugman@cl.cam.ac.uk>
Message-Id: <E13UADd-0006i0-00@wisbech.cl.cam.ac.uk>
```

Captain Phelps:

Thank you for your interest in Iris Recognition.
I will be happy to mail you some scientific papers about this.

In the meantime, you can find a lot of material at this URL:

http://www.cl.cam.ac.uk/users/jgd1000/

... although I have just completed 2.3 million IrisCode comparisons and now I need to publish these updated results. Here is just one graph, summarizing the distribution from those 2.3 million comparisons:

http://www.cl.cam.ac.uk/users/jgd1000/millioncompares.gif

What this shows is that it is "statistically impossible" for two different iris patterns to have a Hamming Distance below about 0.33, which means to disagree in fewer than about 33% of their IrisCode bits. That is the reason why iris recognition decisions are made with such high confidence, even tolerating up to a third of the bits being wrong.

Regards,

John Daugman, Ph.D., O.B.E.
The Computer Laboratory
University of Cambridge
Cambridge CB2 3QG UNITED KINGDOM
tel. +44 1223 334501   fax: +44 1223 334679
Web: http://www.cl.cam.ac.uk/users/jgd1000/

Bibliography

Adler, F.H., Physiology of the Eye, London: The C.V. Mosby Company, 1965

Alexandridis, E., The Pupil, New York: Springer-Verlag, 1985

British Telecommunications, "Iris Recognition - The Technology" n. pag. http://innovate.bt.com/showcase/iris_scanning/index.htm. 17 Jan 2000.

Buda, Gary and Matthew King, Biometrics: Fingerprint Identification System, Defense Technical Information Center, 12 May 1999

Daugman, John, Ph.D., "Advantages and Disadvantages of the Iris for Identification", n. pag. http://www.cl.cam.ac.uk/users/jgd1000/addisadvans.html. 17 Jan 2000.

Daugman, John, Ph.D., "Anatomy and Physiology of the Iris", n. pag. http://www.cl.cam.ac.uk/users/jgd1000/anatomy.html, 17 Jan 2000.

Daugman, John, Ph.D., "Genetic Penetrance and Iris Recognition", n. pag. http://www.cl.cam.ac.uk/users/jgd1000/genetics.html. 17 Jan 2000.

Daugman, John, Ph.D., "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 15, No 11, November 1993

Daugman, John, Ph.D., "Mathematical Explanation of Iris Recognition", n. pag. http://www.cl.cam.ac.uk/users/jgd1000/math.html, 17 Jan 2000.

Daugman, John, Ph.D., "Recognizing Persons by Their Iris Patterns,", Biometrics: Personal Identification in Networked Society, Kluwer, Amsterdam, 1998

Daugman, John, Ph.D., The Computer Laboratory, University of Cambridge, Cambridge, United Kingdom. Personal Correspondence. 19 January 2001

Daukantas, Patricia, Government Computer News, "The service wants to eliminate passwords for verifying users (Sep 27, 1999)" n. pag. http://www.gcn.com/vol18_no32/news/702-1.html. 17 Jan 2000.

Denning, Dorothy E., Information Warfare and Security, Reading, Massachusetts, 1999

Diebold Inc., "Iris Recognition News Release", 13 May 1999, n. pag. http://www2.diebold.com/ficcimg/whatsnews/iris/pr.htm. 17 Jan 2000.

Diebold Inc., "Iris Recognition Questions and Answers" n. pag. http://www2.diebold.com/ficcimg/whatsnews/iris/qa20.htm, 17 Jan 2000.

Encyclopedia Britannica, n. pag. http://www.britannica.com/, 3 Oct 2000

Gifford, M, McCartney, D and Seal, C, British Technology Journal, “Networked Biometrics Systems — Iris Recognition”, Vol. 17 No 2 April 1999

Gruska, Jozef, Foundations of Computing, London: Thomson Computer Press, 1977

Holcombe, Bill, Director, E-Business Technologies, Office of Government wide Policy, “Management Guide to Smart Card Applications:
Issues, Economics and Guidelines for E-Gov Planning & Implementation”, presentation for The Smart Technologies Forum, 18 November 2000

Holcombe, Bill, Director, E-Business Technologies, Office of Government wide Policy. Personal Correspondence. 1 February 2001

IriScan Inc., “How It Works” n. pag. http://www.iriscan.com/html/recognition.html, 14 Jan 2000.

IriScan Inc., “How It Works” n. pag. http://www.iriscan.com/html/recognition2.html. 14 Jan 2000.

IriScan Inc., “Safety Statements” n. pag. http://www.iriscan.com/html/safetystatement.html, 17 Jan 2000.

IriScan Inc., “Scientific Basis for Iris Recognition” n. pag. http://www.iriscan.com/html/basis.html, 14 Jan 2000.

IriScan Inc., “Technology Development” n. pag. http://www.iriscan.com/html/techdev.html, 14 Jan 2000.

Loewenfeld, Irene E, Ph.D., The Pupil, Volume 1, Iowa State University Press, 1993

Merriam-Webster's Collegiate Dictionary, n. pag. http://www.britannica.com/bcom/dictionary/, 1 Nov 2000

Schneier, Bruce, “Internet Cryptography,” 12th Annual First Conference, Chicago, IL, June 2000

Schneier, Bruce, Applied Cryptography, Second Edition, New York: Wiley and Sons, Inc, 1996

Sensar Inc., “Sensar Iris ID: In Use Today” n. pag. http://www.sensar.com/products/prod-customers.stm, 17 Jan 2000.

Shannon, Matt, Government Services Sales Representative, IriScan Inc. Telephone Interview. March 2000

Smart Card Central, “Samsung And Incard Launch World's First 32-bit Smart Card For High-Volume SIM Applications”, n. Pag., http://www.smartcardcentral.com/news/pressrelease/oct2000/samsung_103100.asp, 1 Nov 2000

SmartGov, “Smart Card Technology Center”, n. pag., http://www.smart.gov/techcenter/section04n.htm, 15 January 2001

SmartGov, “Smart Card Technology” n. pag. http://www.smartcard.gov/, 1 November 2000

USA Today Tech Reviews, “New ATM: Look me in the eye and pay that (23 Nov 1999)” n. pag. http://www.usatoday.com/life/cyber/tech/review/crg022.htm. 17 Jan 2000.

Webster’s New Universal Unabridged Dictionary, New York: Barnes & Noble Books, 1996

Yin, Robert K., Case Study Research Design and Methods, London: Sage Publications, 1984

Vita

Captain Orval E. Phelps was born in Jacksonville, North Carolina. He graduated from North Fremont High School in Ashton, Idaho in May 1985. He entered undergraduate studies at the University of Idaho in Pocatello, Idaho in September 1985. He entered the Air Force in March 1986 as an enlisted computer programmer. He again entered undergraduate studies at Troy State University Montgomery in Montgomery, Alabama where he graduated with a Bachelor of Science degree in Computer and Information Science in June 1995. He was commissioned through Officer Training School at Maxwell Air Force Base, Alabama in January 1996.

His first assignment in the Air Force was at Gunter AFB as an enlisted computer programmer assigned to the Standard Systems Group in May 1986. In October 1995, he was assigned to Officer Training School as an officer trainee. In January 1996, he was assigned to the Headquarters Air Force Personnel Center, Directorate of Assignments, Randolph AFB, Texas where he served as the Chief, Assignment Management Systems Section. In August 1999, he entered the Graduate Information Resource Management program, School of Systems Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be assigned the 99th Communications Squadron, Nellis Air Force Base Nevada.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** 20-03-2001	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE

Information Security: Securing Smart Cards with Iris Recognition

5. FUNDING NUMBERS

6. AUTHOR(S)

Orval E Phelps, Captain, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Instutute of Technology
2750 P Street
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENG/01M-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

William O. Holcombe
GSA - ME Rm G-131
18th & F St NW
Washington, DC 20405

bill.holcombe@gsa.gov
202-208-7657

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

Advisor: Henry B Potoczny, Ph. D.
2950 P St, WPAFB, OH 45433-7765
DSN 785-6565 x4282
email:Henry.Potoczny@afit.af.mil

12a. DISTRIBUTION AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This thesis examines the application of iris recognition technology to the problem of keeping smart cards secure. In order to understand the technology, a comprehensive literature review was conducted. The biological components of the iris were examined to ensure that they were truly random in development and static through the lifetime of the individual. Specifically, the physical structure of what comprises the iris was examined in detail. The data gathered indicates that the iris is formed early in development, random in structure, and stable throughout the person's lifetime. Next, the iris recognition process and resulting recognition code was examined to determine how it could be used. Examination of methods to eliminate counterfeit codes and the randomness of independent codes was vital. Statistics on reliability of the iris recognition process were also examined. Iris recognition was found to be exceptionally reliable, difficult to counterfeit and fast to use. In order to ensure security, the cryptographic strength of the iris recognition code was examined. It was necessary to determine the time necessary to break the iris recognition code should the smart card be compromised. Due to the randomness of the code, exhaustive searches are the only viable means of breaking the code and the time durations to accomplish this are excessive. Additionally, smart card technology was examined to determine if existing technology could store the necessary iris recognition information for use in identity verification. Current processing ability and storage requirements of smart cards exceed the minimum requirements for use of iris recognition technology. The conclusion of this thesis is that iris recognition technology is a viable means of securing smart cards against unauthorized access with high

14. SUBJECT TERMS Iris Recognition, Smart Cards, Case Study Methodology, Information Security	**15. NUMBER OF PAGES** 57
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL